AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for establishing a network connection between a first machine and a second machine, comprising:

determining suspicious network activity on the network;

if suspicious network activity is determined, establishing a first communication session between the first machine and a monitoring device;

after establishing the first communication session, receiving by the monitoring device ~~an initial packet~~ a data access request from ~~a~~ the first machine ~~for establishing a communication session between the first machine and a second machine~~;

storing the data access request;

sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; ~~and~~

after a valid response to the test is received, establishing ~~the~~ a second communication session between ~~the first and~~ the second ~~machines~~machine and the monitoring device ~~after a valid response is received to the test.~~ ; and

after establishing the second communication session, forwarding the data access request from the monitoring device to the second machine.

2. (Currently Amended) The method of claim 1, wherein the establishing the first communication session ~~further comprising~~ comprises receiving by the monitoring device from the first machine an initial packet, and responding to the initial packet ~~from the first machine~~ by sending from the monitoring device a response packet to the first machine encoding a connection state for establishing the communication session.

3. (Original) The method of claim 2 wherein the initial packet is a SYN packet in accord with the TCP protocol and the response packet is a SYN ACK packet in accord with the TCP protocol.

4. (Currently Amended) The method of claim 3, wherein the SYN ACK packet comprises a number encoding a first address for the first machine on the network, and a second address for the second machine on the network.

5. (Currently Amended) The method of claim 2, wherein responding to the initial packet by sending the response packet comprises:

generating a number to be included in the response packet by encrypting ~~the connection state of the response packet comprises a number encoding~~ a first address for the first machine on the network, a second address for the second machine on the network, and a secret unknown to the first machine, ~~the number to facilitate validating~~ facilitating validation of an acknowledgement packet from the first machine responsive to the response packet.

6. (Currently Amended) The method of claim [[1]]5, further comprising:

receiving ~~an~~ the acknowledgement packet from the first machine responsive to the encrypted response packet;

decoding a tentative connection state information from the acknowledgement packet; and

determining if the tentative connection state information is valid.

7. (Original) The method of claim 1, further comprising:

preparing a web page embodying the test; and

said sending the test to the first machine including sending the web page to a networking application program of the first machine, the networking application program operative to receive and display the web page.

8. (Original) The method of claim 1, wherein the test is embodied within a web page.

9. (Cancelled)

10. (Currently Amended) The method of claim [[1]]10, ~~further comprising: monitoring by a monitoring device of attempts to establish communication sessions with the second machine;~~wherein the establishing the third communication session between the first and second machines includes the monitoring device storing an identifier for the first machine in a list identifying machines that have provided the valid response.

11. (Currently Amended) A method for a monitoring device to facilitate communication between a client and a protected server, comprising:

receiving a first packet from the client to begin a handshake for establishing a first network connection between the client and the ~~intermediary;~~monitoring device

sending a second packet to the client to acknowledge the first packet;

receiving a third packet from the client acknowledging the second packet;

receiving a data access request from a networking application program of the client; ~~and~~

storing the data access request;

sending by the monitoring device a test to the networking application program, the test having at least one characteristic making the test resistant to automatic answering of the ~~test.~~test;

after a valid response to the test is received, establishing a second network connection between the protected server and the monitoring device; and

after establishing the second communication session, forwarding the data access request from the monitoring device to the protected server.

12. (Currently Amended) The method of claim 11, further comprising:

receiving a response to the test from the client;

determining the response comprises a valid answer to the test; and

~~establishing a second network connection between the monitoring device and the protected server; and~~

facilitating communication between the client and the protected server.

13. (Original) The method of claim 11, wherein the monitoring device does not allocate resources for tracking a state information for establishing the first network connection and instead encodes the state information within the second packet.

14. (Original) The method of claim 11, wherein the third packet encodes a known alteration of the state information.

15. (Original) The method of claim 11, wherein the data access request is a GET request formatted with respect to HyperText Transport Protocol (HTTP).

16. (Original) The method of claim 11, wherein the networking application program includes a web browser, and the test comprises a web page incorporating the test.

17. (Currently Amended) A system, comprising:

a protected server responsive to network connection requests;

a client machine seeking to establish communication with the protected server; and

a monitoring device communicatively interposed between the protected server and the client machine, wherein the monitoring device is configured to store a data access request from the client machine, to send a test resistant to automatic answering to the client machine, and to forward the data access request from the monitoring device to the protected server for ~~to~~ facilitat~~e~~ing establishing ~~the client machine~~

communication ~~with~~between the client machine and the protected server if a valid response to the test is received by the monitoring device.

18. (Original) The system of claim 17, wherein the monitoring device is further configured to perform:

receiving an initial packet from the client machine for establishing a communication session; and

responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session.

19. (Currently Amended) An article comprising:

a machine-accessible ~~media~~storage medium; and

~~having associated~~ data stored in the storage medium, wherein the data, when accessed, results in ~~a machine~~ an apparatus communicatively coupled with a network to facilitate communication between a first machine and a second machine by performing:

determining suspicious network activity on the network;

receiving ~~an initial packet~~ a data access request from ~~a~~ the first machine ~~for establishing a communication session between the first machine and a second machine~~;

storing the data access request;

sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and

after a valid response to the test is received, forwarding the data access request from to the second machine~~establishing the communication session between the first and second machines after a valid response is received to the test~~.

20. (Original) The article of claim 19 wherein the machine-accessible media further includes data, when accessed, results in the machine performing:

receiving an initial packet from the first machine for establishing a communication session; and

responding to the initial packet from the first machine by sending a response packet to the first machine encoding a connection state for establishing the communication session.

21. (Currently Amended) An article ~~comprising~~ comprising:

a machine-accessible ~~media~~storage medium; and

~~having associated~~ data stored in the storage medium adapted to enable a monitoring device to facilitate communication between a client and a protected server, wherein the data, when accessed, results in ~~a machine~~the monitoring device performing:

receiving a first packet from the client to begin a handshake for establishing a first network connection between the client and the ~~intermediary~~monitoring device;

sending a second packet to the client to acknowledge the first packet;

receiving a third packet from the client acknowledging the second packet;

receiving a data access request from a networking application program of the client; ~~and~~

storing the data access request;

sending by the monitoring device a test to the networking application program, the test having at least one characteristic making the test resistant to automatic answering of the ~~test~~ test;

after a valid response to the test is received, establishing a second network connection between the monitoring device and the protected server; and

after establishing the second network connection, forwarding the data access request from the monitoring device to the protected server.

22. (Currently Amended) The article of claim 21 wherein the machine-accessible media further includes data, when accessed, results in the machine performing:

receiving a response to the test from the client;

determining the response comprises a valid answer to the test; and

~~establishing a second network connection between the monitoring device and the protected server; and~~

facilitating communication between the client and the protected server.

23. (New) The method of claim 1, wherein the determining the suspicious network activity comprises:

tracking by the monitoring device a number of attempts to establish communication sessions with the second machine; and

if the number of attempts exceeds a predetermined threshold per a predetermined time period, modifying a state of the monitoring device from a normal mode of operation to a safe mode of operation.

24. (New) The method of claim 23, further comprising:

if the number of attempts falls below the predetermined threshold, modifying the state of the monitoring device from the safe mode of operation to the normal mode of operation; and

while in the normal mode, facilitating by the monitoring device establishing of communication sessions directly between the first machine and the second machine.

25. (New) The method of claim 1, further comprising after a valid response to the test is received and the second communication session is established, facilitating by the monitoring device establishing of a third communication session directly between the first machine and the second machine.

26. (New) The method of claim 1, wherein the test is sent to the first machine by the monitoring device.

27. (New) The method of 1, wherein the data access request is a GET request formatted with respect to HyperText Transport Protocol (HTTP).